**Group Insurance Regulations**
**Administrative Supplement No. 19**
**April 2003**

# University of California Group Health and Welfare Benefit Plans HIPAA Privacy Rule Policies and Procedures (Interim)

The University of California's Systemwide HIPAA Standards and Implementation Policies require all covered entities within the University to establish policies and procedures implementing the HIPAA Privacy Rule (Privacy Rule). The University's Self-funded Medical Plans and the Health Care Reimbursement Account (HCRA) program are defined under HIPAA as covered entities. In addition, certain University insured health plans are defined under HIPAA as covered entities. For the purpose of the privacy protection portions of these policies and procedures, the HIPAA covered self-funded and insured plans will be treated the same. The following policies and procedures for the Privacy Rule define actions that must be implemented to meet the requirements of the UC Systemwide HIPAA Standards, and describe what specific departmental policies and procedures should address.

It is the policy of the University that all University employees who work with its HIPAA covered insured and self-funded plans will protect the privacy of individual health information and maintain the security of protected health information (PHI). The University will provide members rights to;

- request access to their PHI,
- request the modification of their PHI, and
- request restricted use of their PHI.

Upon request, the University will also provide an accounting of disclosures of an individual's PHI. The University will provide these rights as follows:

- For the insured medical plans, only the PHI that the University holds; and
- For the self-funded plans, both the PHI that the University holds and the PHI held by the University's applicable Business Associate.

## 1. Who Must Comply

Any employee or entity that provides services or assists the Group Health and Welfare Benefit Plans in activities that involve the use and disclosure of protected health information (PHI) must comply with the following policies and procedures.

## 2. Protected Health Information (PHI)

Protected Health Information (PHI) is a member's health information that:

1. Is created or received by a health care provider, plan, or clearinghouse;
2. Relates to the past, present or future physical or mental health or condition of a member, the provision of health care to the member, or the past, present or future payment for the provision of health care to the member;
3. Identifies the member, or is reasonably believed could identify the member; and
4. Is transmitted or maintained in any form or medium.

The following information associated with the health plan should be considered PHI:

1. Name;
2. All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census;
   (a) The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and
   (b) The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people are changed to 000.
3. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;
4. Telephone numbers;
5. Fax numbers;
6. Electronic mail addresses;
7. Social security numbers;
8. Medical record numbers;
9. Health plan beneficiary numbers;
10. Account numbers;
11. Certificate/license numbers;
12. Vehicle identifiers and serial numbers, including license plate numbers;
13. Device identifiers and serial numbers;
14. Web Universal Resource Locators (URLs);
15. Internet Protocol (IP) address numbers;
16. Biometric identifiers, including finger and voiceprints;
17. Full face photographic images and any comparable images; and
18. Any other unique identifying number, characteristic, or code.

## 3. Use and Disclosure of PHI

PHI may be used or disclosed without authorization only for Treatment, Payment and Health Care Operations.

- **Treatment:** Provision, coordination or management of health care by a provider.
- **Payment:** Activities that involve reimbursement for health care, such as determination of eligibility or coverage, claims processing, billing, obtaining and payment of premium, utilization review, medical necessity determinations, health care data processing, and precertifications.
- **Health Care Operations:** Certain health care operations assure that all UC enrollees receive quality care. PHI will be used when needed for plan administration, planning, data analysis, utilization review, quality assurance, benefit management, practice management, referrals to specialists, or legal, actuarial, accounting, consulting, data aggregation, management, administrative or financial services.

## 4. Creating a Firewall

In order to comply with the requirements of HIPAA, these Policies and Procedures must create a firewall between covered functions (the University's Group Health and Welfare Benefit Plans), and non-covered functions (such as employer related functions not associated with the University's Group Health and Welfare Benefit Plans). Member PHI can not be used or disclosed for employment-related actions or decisions; nor may it be used or disclosed in connection with any other benefit or employee benefit plan of the University. Workforce members engaged in multiple roles, including the use and disclosure of PHI, must keep PHI separate from other job responsibilities. Any disclosure of PHI between the covered and non-covered functions will require the member's written authorization, in most cases.

If your department deals with the Group Health and Welfare Benefit Plans and employment-related functions, you must:

- Keep PHI in confidential files separate from employer-related files;
- Maintain a strict separation of function between Health and Welfare Benefits and employment related functions; (For example, you cannot use information you learned about a member while helping them with a health claim to make employment related decisions.)
- Review internal security measures to safeguard the firewall between these functions;
- Consult with your supervisor or local privacy officer if you have HIPAA compliance questions, are reporting violations of this firewall, or require procedural assistance.

## 5. Minimum Necessary

Use the "minimum necessary standard" when accessing or using PHI. "Minimum necessary" means using only the minimum amount of member information needed for Treatment, Payment and Health Care Operations. Use or disclosure of PHI should only be the minimum amount necessary to accomplish the intended purpose. For example, do not share a member's Social Security number if this information is not needed to get the job done. Employ a "think twice" standard asking:

- Is it reasonable?
- Is it necessary?

It is the responsibility of each department to ensure that access to PHI is based on those who need access to the information to do their jobs. Department practices should be evaluated to enhance safeguards as needed to limit unnecessary or inappropriate access to and disclosure of PHI.

## 6. Written Authorizations

Written member authorization must be obtained prior to use or disclosure of PHI that falls outside the scope of Treatment, Payment and Health Care Operations, unless otherwise required by law or permitted by HIPAA. For example, an authorization must be obtained before sharing PHI for employment related purposes. Exceptions to the need for a written authorization are listed in the GIR Preface Provision E, Section I.

The Office of the General Counsel, in consultation with the HIPAA Taskforce, has developed a model Authorization Form (Attachment #2) that includes all the required elements of a valid HIPAA authorization. A valid Authorization must include an identification of the PHI to be used or disclosed, by whom (name or class of person), to whom, and an expiration date. The Authorization must also include the following notifications to the individual:

1. The individual may revoke the Authorization in writing and indicate how to do so;
2. Treatment, payment, enrollment or eligibility for benefits may not be conditioned on an Authorization;
3. PHI may be redisclosed by the person receiving the PHI, and in that case, the confidentiality of the PHI is no longer protected.

## 7. Member Rights

The Privacy Rule gives members a right to be informed of the privacy practices of their health plan, as well as to be informed of their privacy rights with respect to their PHI. The University must provide all members who receive health care from a self-funded

medical plan or reimbursements from the Health Care Reimbursement Account with the Notice of Privacy Practices (Attachment #1).

Under the HIPAA Privacy Rule members may exercise the following rights regarding their PHI:

- The right to receive a copy of the covered entity's notice of privacy practices;
- The right to inspect and copy their PHI;
- The right to request amendment of their PHI;
- The right to request an accounting of disclosures of PHI for purposes other than Treatment, Payment or Health Care Operations;
- The right to request that uses and disclosures of PHI be restricted.

Members may exercise these rights or register a complaint by submitting a request in writing to the UC Health and Welfare Plans, Privacy Liaison at:

Attn: Privacy Liaison
University of California
Office of the President
Human Resource and Benefits
300 Lakeside Drive, 5th Floor
Oakland, CA. 94612-3557

Phone Number: 1-800-888-8267 ext. 7-3857
(510) 287-3857

- A response to written requests, approving or denying access will be made within 30 days.
- Action granting access or denial of access will take place within 60 days if the designated record set is located or maintained off-site and not readily accessible.
- If the Health Plan or HCRA program does not maintain the designated record set, a written response will be sent to the requesting member.

## 8. Training

The Privacy Rule requires training of all University workforce members working with the University's self-funded medical plans and Health Care Reimbursement Account, regarding policies and procedures with respect to HIPAA and PHI. Additionally, in order to receive PHI for member advocacy and plan administration purposes, UC has certified to its HIPAA-covered insured plans that its workforce has been trained in the policies and procedures pertaining to privacy protection. This includes subsequent training of new staff and retraining as changes occur within both HIPAA and UC policies and procedures. Documentation of the training must be kept in written or electronic form for six years. For purposes of determining the scope of the training required, UC has defined all those who work or volunteer within the classes of employees in GIR Preface Provision

E Section III, as employees who need to be trained in the HIPAA policies and procedures.

Supervisors will be responsible for ensuring that workforce members are appropriately trained in these policies and procedures. Workforce members will be trained soon after they join the University, but no later than 90 days. When significant changes occur in the job description of current employees or policy and/or procedures, the affected workforce members will be trained as soon as possible after such changes. Records documenting the required training will be kept in the Human Resources Office at each University location.

## 9. Safeguarding PHI

It is the policy of the University to protect PHI and ensure compliance with HIPAA Privacy Rule requirements. Workforce members are legally and ethically responsible to protect the privacy and confidentiality of a member's PHI. For assistance to address PHI concerns you may contact your supervisor, the location's Privacy Officer or Legal Counsel, the Health and Welfare Privacy Liaison, the University's Privacy Official or the UC Office of The General Counsel.

Resources to assist UC's workforce members in achieving compliance with the HIPAA Privacy Rule include;

1. The University's Systemwide HIPAA Standards and Implementation Policies, (website)
2. The Group Insurance Regulations (GIRs) Preface Provision E including this Group Health and Welfare Benefit Plans HIPAA Polices and Procedures Supplement, (GIRs)
3. The approved legal documents and forms:
   a. Notice of Privacy Practices, (attachment #1)
   b. Authorization Form, (attachment #2)
4. Power Point Training Modules, (website)
5. University HIPAA Privacy Website.

Recommended PHI safeguards to consider include:

- Know the additional privacy practices and policies specific to your department;
- Protect confidential information from unauthorized access, use or disclosure;
- Maintain physical security, access control, locked storage as appropriate;
- Do not leave PHI unattended in public view;
- Never dispose of paper or items containing member PHI in the regular trash;
- Confidential information should never be discussed in public areas, such as hallways, cafeterias, or restrooms;

- Report known or suspected violations of privacy;
- Computer passwords are unique, do not share your password or log on a computer for someone else;
- Stop and question individuals who do not belong in your work area,
- Never remove paper or items containing member PHI from the facility unless authorized to do so.
- Implement ways of verifying who you are talking to, for example, you may want to ask for three personal identifiers such as the last four digits of the member's social security number, the member's date of birth, and if a retiree, the UC location the member retired from. It is also a good idea to establish a similar protocol within your department before sharing PHI with family members.

Accessing or communicating PHI not associated with job responsibility is considered a violation of this policy and may result in corrective action.

In the event of improper use or disclosure of PHI, the following mitigation efforts should be made:

- Contain the damage and stop further use or disclosure;
- Utilize violations as a means to identify system lapses and to modify policies or procedures;
- Inform members, where appropriate, of any improper use or disclosure arising from a violation of HIPAA regulations.

## 10. Facsimile of PHI

This policy provides guidance on the appropriate use of facsimile (fax) transmission of information to ensure the confidentiality and security of PHI.

Recommended fax safeguards to consider include:

- Verify accuracy of fax numbers with intended recipient before sending a fax;
- When faxing for someone else, don't change the fax number without consulting the sender;
- Use fax cover sheets;
- Notify facilities that you commonly receive faxes from if your number changes;
- Double check the fax number before sending the fax;
- Recipients you commonly fax information to should be pre-programmed;
- When faxing PHI, verify fax number and availability of recipient prior to sending, and verify receipt;
- Place a reminder over the fax machine of process to follow when faxing PHI;
- Locate machines out of public view;
- Establish a routine for regular removing/distribution of incoming faxes.

Pre-programmed Fax Numbers:

- Use pre-programmed numbers whenever possible;
- Pre-program number and send test fax requesting verification of receipt.

Fax Cover Sheet Requirements:

- Completed cover sheets with standard confidentiality statement and disclaimer are required on all organizational fax transmissions of PHI.

  Sample fax wording:

  "This fax is intended only for the use of the individual or entity to which it is addressed and may contain information that is confidential and prohibited from disclosure. If you are not the intended recipient, you are hereby notified that any dissemination, or copying of this message, or any attachment, is strictly prohibited. If you have received this fax in error, please notify the original sender immediately by telephone or by return fax and destroy this fax and any copies. Thank you"

Misdirected Faxes:

- Obtain the fax number of the unintended receiver and immediately transmit a request that the material be destroyed immediately or retrieved by mail or delivery. If fax contained PHI, notify a supervisor, log the disclosure.

## 11. Computer Safeguards

Recommended computer safeguards to consider include:

- Do not share your computer passwords with anyone;
- Do not leave your passwords posted or attached to your computer or easily visible on your desk;
- Make sure computer screens are not visible to passersby;
- Use Privacy screens whenever possible;
- Log off your computer when you are done, or if you walk away from the computer for a period of time;
- If possible, use automatic time-outs or screen savers to protect the information from being easily visible;
- Do not allow any individual to use your terminal after your have signed in; (Any information changed/altered or accessed can be traced back to your login, and you will be held responsible for the PHI that was altered or accessed.)
- Email messages transmitting PHI should include a brief confidentiality statement and disclaimer.

  Sample email wording:

  "This message, together with any attachments, is intended only for the use of the individual or entity addressed and may contain information that is confidential

and prohibited from disclosure. If you are not the intended recipient, you are hereby notified that any dissemination, or copying of this message, or any attachment, is strictly prohibited. If you have received this message in error, please notify the original sender immediately by telephone or by return email and delete this message along with any attachments, from your computer. Thank you"

## 12. Consequences of Violating the HIPAA Privacy Rule

It is the University's policy to prevent unauthorized or unapproved access to or disclosure of member PHI. Report any concerns to your supervisor or the Privacy Officer at your location.

An incidental use or disclosure of PHI is not permitted if it is a byproduct of a primary use or disclosure that is a violation of the Privacy Rule. If a federal Department of Health and Human Services (DHHS) investigation concluded that disclosure was intended and/or reasonable safeguards did not exist, the covered health plans or UC workforce could be subject to substantial sanctions or fines. For example, you may leave messages on a member's answering machine, but should take care to limit the amount of information disclosed and use your judgment to assure that such disclosures are in the best interest of the member. The member has a right to request confidential communications, and if the member has requested a restriction on voicemail messages, you must comply. Failure to honor that request and continuing to disclose PHI on voicemail could be a violation of the Privacy Rule.

HIPAA also imposes penalties and fines for breaches of privacy. Breach of University policies can result in the application of progressive discipline procedures. External investigations of violations can result in serious penalties. For example, an individual found guilty of releasing confidential information for personal gain (such as selling information about a celebrity to a newspaper) could be fined $250,000 and be imprisoned for 10 years.